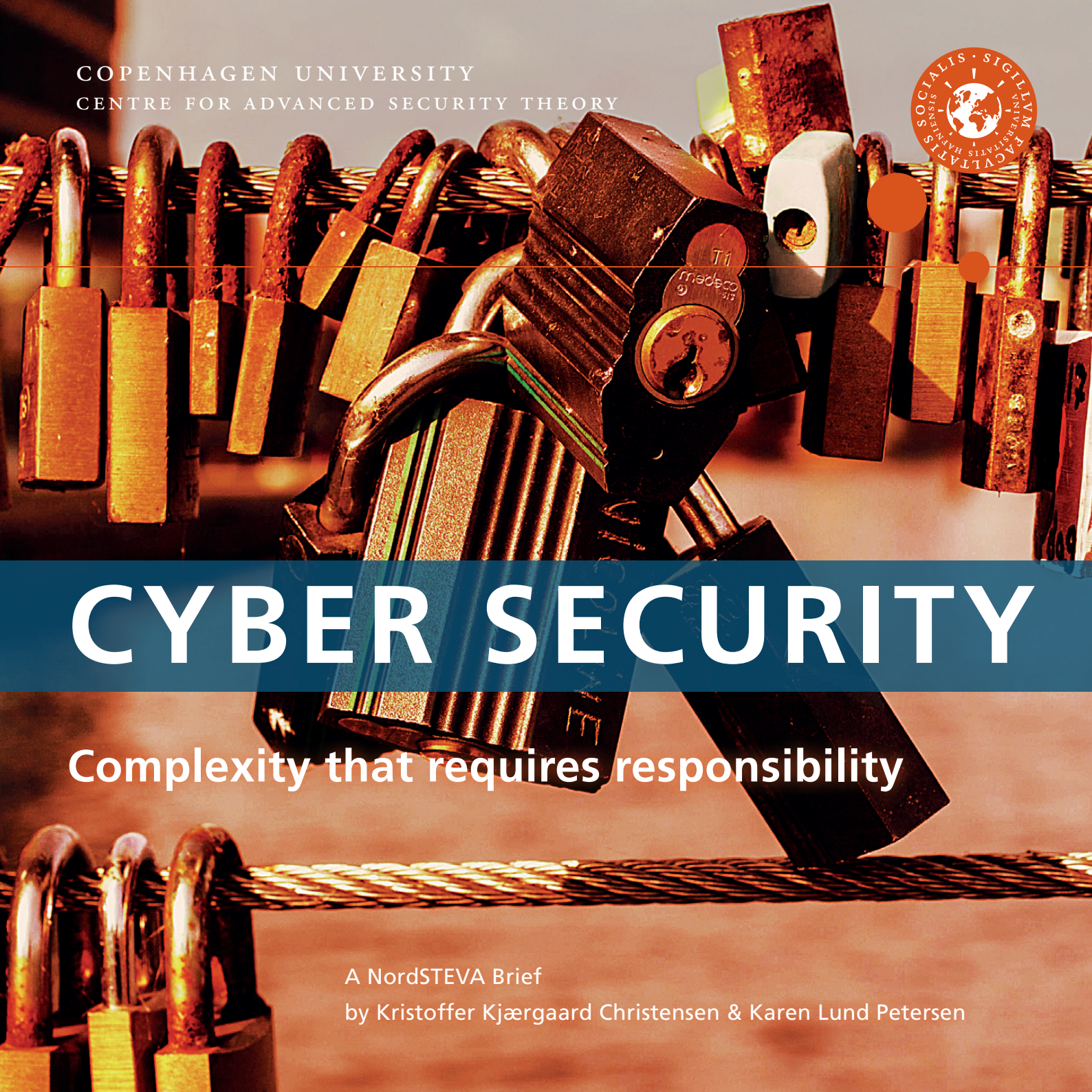
Cyber Security

Complexity that Requires Responsibility

Christensen, Kristoffer Kjærgaard; Petersen, Karen Lund

Publication date:
2017


COPENHAGEN UNIVERSITY
CENTRE FOR ADVANCED SECURITY THEORY
SOCIALIS · SIGILLVM FACVLTATIS SCIENTIARVM HAFNIENSIS
CYBER SECURITY
Complexity that requires responsibility
A NordSTEVA Brief
by Kristoffer Kjærgaard Christensen & Karen Lund Petersen

Cyber security is considered the absolute largest security challenge amongst both private companies and public authorities. Responsibility for national cyber security is however divided between companies, civil society organizations and governments, and there is hence a great deal of confusion as to who should do what and when. This paper outlines the current challenges to Western companies and provides recommendations for how companies can best address future cyber threats.

RECOMMENDATIONS

- Create a space for prioritization and strategic thinking in relation to cyber threats.
- Be active in public debates on cyber security management and legislation, and start to develop common business standards and norms in this area.
- Focus on organizational learning and training to ensure dialogue and constructive "translation" between the strategic and the technical levels.

Several studies show that private companies – regardless of sector – today consider the threat to and through information and communication technologies (ICT or cyber threats) the absolute greatest challenge. US and European intelligence services also consider cyber threats as a global challenge, and NATO has recently designated cyberspace as an independent domain of warfare.

Despite this consensus on the importance of the problem, there is far from an agreement on the resources needed to combat the threat. The complex, dynamic and diffuse character of the threat makes it intangible and thus difficult to control. Information and communication technology is everywhere: It not only transcends national jurisdictions but has found its way into the 'private space' in the digital age. Our critical infrastructure, private companies and the most intimate aspects of our daily lives are influenced by information and communication technologies and the rapidly growing 'Internet of Things'.

This development drastically increases security vulnerabilities and the number of potential targets – from states to private companies and individual users. We do not know where the cyber threat comes from or who/what will be the target. Is it states or individuals who attack? Is it guided by political or economic motives – or perhaps something entirely different? This uncertainty makes classical political governance through legislation very difficult. Combating cyber threats instead requires security policies that transcend our classic divisions between police and defense.

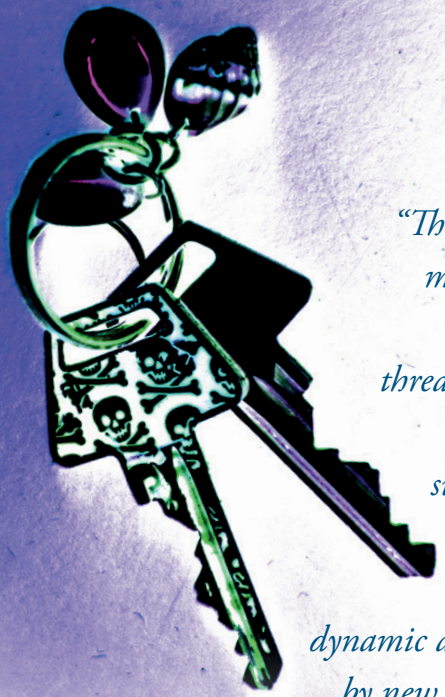
In brief, to effectively fight cyber threats voluntary contributions and active efforts from companies and organizations is required. It is no longer enough for private actors to relate to new legislation. Rather the nature of the threat requires social responsibility and self-regulation in a wide range of organizations across society. More than ever, we see an erosion of the boundaries between the state's responsibility for national security and the citizen's right to protection; between the public and the private sphere.

In the following, we will outline the challenges facing Western companies in relation to cyber threats and provide three suggestions for how companies can and should take action.

"Cyber/Communications Security remains the greatest security concern facing Fortune 1000 companies in 2016",

2016 Survey of Fortune 1000 Companies, Securitas

WHAT IS THE TASK FOR PRIVATE BUSINESS?



"The difference is a more diffuse and unpredictable threat scenario than previously. The surface of attack related to IT is hyper dynamic and is increased by new technologies, as well as the expectation that our digital identity is available 24/7/365 - no matter where we are in the world".

Thomas Baltzer Jensen, Chief Risk Officer,
the Danish National Bank

It is generally difficult to distinguish between various ICT-related security breaches, such as advanced, state-sponsored hacker attacks, computer theft, vandalism and technological failure. It is associated with great difficulties and considerable costs to determine who and where the threat comes from. Because this analysis is often difficult and very expensive, it is also not always in the interest of companies or organizations to carry out a thorough analysis of an incident in order to identify the actors behind. For private businesses, it is much more relevant to assess their own vulnerabilities and the consequences that an attack may have for future operations, projects and reputation. In private companies there is thus less focus on threatening actors and more focus on the methods and vulnerabilities associated with an incident.

For the most part, vulnerabilities and ICT-related threats are considered an inevitable condition of doing business that can be mitigated by ensuring secure systems and workflows, as well as through risks assessments of new business initiatives – all of this in accordance with the individual company's strategic priorities and risk appetite. Although much of this is also true for public organizations and government agencies, companies do diverge in some important respects.

Many companies operate globally and therefore do not only look at threats to their national networks. Rather, they need to consider the broader landscape of political risks. Thus, national borders do not define their cyber threats. Therefore, companies cannot solely rely on cooperation with the authorities in determining the threat level and in setting the necessary security standards. Companies need to do the analysis themselves and take initiatives in this area.

Although the companies' own procedures and techniques may potentially be secured and technically improved, there are still some basic strategic challenges. As a

study by PwC shows, companies consider the threat from organized criminal hackers to be the greatest – primarily due to the potentially large financial losses. Cyber security legislation is of a lesser concern (See e.g. PwC's Cyber Crime Survey 2016). However, this view on legislation and regulation is expected to change in the coming years; partly because of the intensified EU efforts in the field of personal data protection, and partly because of the fear of what is commonly know as 'cyber nationalism'. The concept of cyber nationalism points to the tendency amongs governements around the world to establish nationally controlled borders for data handling and protection.

The consequences of such policies are potentially negative for companies operating on the global market. As the literature often highlights, national cyber security laws are not always compatible, and it can therefore be difficult to establish a common practice for the use of technologies. For example, Russia has adopted an antiencryption act (Yarovya Law of 2016), which imposes requirements on companies that are in conflict with European and US privacy protection rules.

In addition to the compatibility issues, certain types of legislation and technological solutions may potentially have farreaching implications for entire sectors. Ecommerce and the telecommunications industry are obvious examples. A good example is the debate about whether intelligence services should have access to a 'backdoor' to encrypted content or information logs from telecommunications companies and ISPs. This kind of access could have farreaching consequences for telecommunications and technology companies and their users worldwide.

We are faced here with a classic dilemma between security on the one hand and privacy (and prosperity) on the other – with companies at the center. How much security should we pursue through surveillance and legislative initiatives? And how much freedom and free trade are we willing to give up in the name of the security? As mentioned below, it is important that companies address these issues and actively participate to have a voice in the debate.

In addition to pointing to the challenges from increased cybercrime, PwC's surveys show that many of the respondents demand clearer priorities from senior management. In the United States 75% say that cyber security is not considered a matter for the board. Instead cyber threats are generally seen as a 'management' issue to be handled in the IT, Security and HR departments. This causes problems with 'silo thinking' and lack of strategic thinking about the nature and extent of the problem.

"Security is not simply a CIO, CSO, or IT department issue... It is a responsibility that must be shared amongst all employees, and CEOs and board members must proactively mitigate future challenges."

AT&T Vice Director, John Donnovan 2015

WHAT CAN BE DONE?

The challenges that the companies face are thus many. While precaution and resilience are the common answers to how we can and should relate to new and more unpredictable threats, it is important to keep in mind that we neither can - nor should - pursue 100% security. This would fundamentally challenge our belief in privacy and the right to self-determination. Instead we must act wisely within the framework of our liberal democracy.

In the following, we highlight three areas where companies and organizations can and should intervene to navigate the new threat landscape.

RECOMMENDATION 1.
PRIORITIZE AND THINK STRATEGICALLY THROUGHOUT THE ORGANIZATION

Due to the complexity of cyber threats, they often affect the entire organization; IT security, corporate security, risk management, CSR and HR. This complexity makes strategic decisions and priorities at the top management level vital. Decisions on cyber and information security at a strategic level ensures the integration of security decisions in everyday business of the organization.

The nature of a 'cyber risk decisions' is, however, not easily comparable to other types of risks. The high level of uncertainty associated with cyber threats makes it nearly impossible to calculate probabilities and consequences of cyber incidents. The task is therefore not to calculate and comply, but to make informed choices based on various possible future scenarios. Risk management in relation to cyber threats thus requires political and strategic choices.

This is not necessarily about increasing funding, but about creating a framework for a more holistic approach to cyber and information security work. The organization's priorities and strategy must be clear. One advice could be to design processes across the entire organization that ensure integration and reflection in relation to the different parts of the organization. This process will not only contribute to the appropriate kind of risk management, but also to avoid compartmentalized thinking on these issues, within the Security, Risk, IT and HR departments. The latter is generally an obstacle to finding cyber- and information security solutions.

RECOMMENDATION 2.
TAKE OWNERSHIP OF POLITICAL DEVELOPMENT

Due to the national security aspect of many cyber threats, the political pressure on organizations and businesses is high – and is expected to increase. Especially for larger companies, such public focus and links to national security can have important reputational impact.

In addition, the area is so central to the future opportunities of companies and organizations for action that it is not advisable to hold off in relation to legislation and norm development in the area. Through cooperation across industries it is possible to set common industrial standards for dealing with threats – outside the political system – and thus be both agenda-setting and prepared. A good example of this is the work of major technology companies in shaping the agenda on transparency and the principles for responding to government requests for data.

As mentioned above, cyber nationalism is a threat to free trade and a matter that, by all accounts, will become increasingly relevant in the coming years. In line with initiatives on norm building in other areas, it is also possible to establish voluntary standards and norms on cyber threats across national borders to help avoid overregulation. The use of voluntary reporting and control systems has become widespread in other areas as a tool for self-regulation. Sustainability goals and Corporate Social Responsibility reports are just a few examples of such important tools for communicating and managing new and unpredictable risks. Another possibility is to increase the use of standards, such as the ISO 27000 standards.

These reporting systems and self-imposed rules are currently regarded as norms that define responsible companies. Although CSR reporting is often criticized for simply being a way of showing all the good things being done, rather than a core activity in the companies, CSR is still an important norm that forces businesses to defend their actions morally.

In relation to cyber threats, companies and organizations can advantageously build upon their existing international collaborations in their efforts to counter the trend towards cyber nationalism. In Denmark there has, for example, recently been an initiative in the financial sector towards norm regulation in the cyber area in the Nordic region – the so-called Nordic Financial CERT. Overall, dynamic technology development gives greater scope for companies to influence the agenda, in contrast to the much slower nature of regulation.

RECOMMENDATION 3.
CREATE OPPORTUNITIES FOR KNOWLEDGE-SHARING AND COMPETENCE DEVELOPMENT

Cyber and information security often appears as difficult technical issues that are nearly incomprehensible to people outside certain specialized circles. This creates a sense of helplessness that must be dealt with. Therefore, and in order for all other goals to be met, it is important that a learning environment in relation to cyber and information security is created. This needs to be a learning environment that promotes dialogue and sound political, economic and strategic thinking. Two steps are necessary:

First, it is essential to ensure the presence of the right competencies in the organization. Strategic and economic, technical and operational competencies are all necessary in order to navigate the complex reality of cyber and information security.

Second, there is in particular a need for translation competencies within the organization to enable the translation of concrete, technical and operational challenges to the strategic level – and vice versa. This is not so much a question of managers, CEOs and board members having technical/operational skills. It is also about making the technical staff understand how their choices and decisions relate to the strategic ones. This enables them to provide an informed basis for the strategic course in the company. In other words, translation and knowledge-sharing are essential to ensure the coherence between strategic and operational decisions.

Last, but not least, there is a need for a greater degree of information-sharing between the organizations. Through cooperation there is a real opportunity to strengthen the knowledge and skills of organizations. Enhanced information-sharing also requires private initiative and strengthening of existing private networks.

"Boards can hold executive management accountable for evaluating current cyber-security risks and maintaining response plans by making cybersecurity debriefings a regular agenda item at board meetings."

Harvard Business Review 2017

May 2017

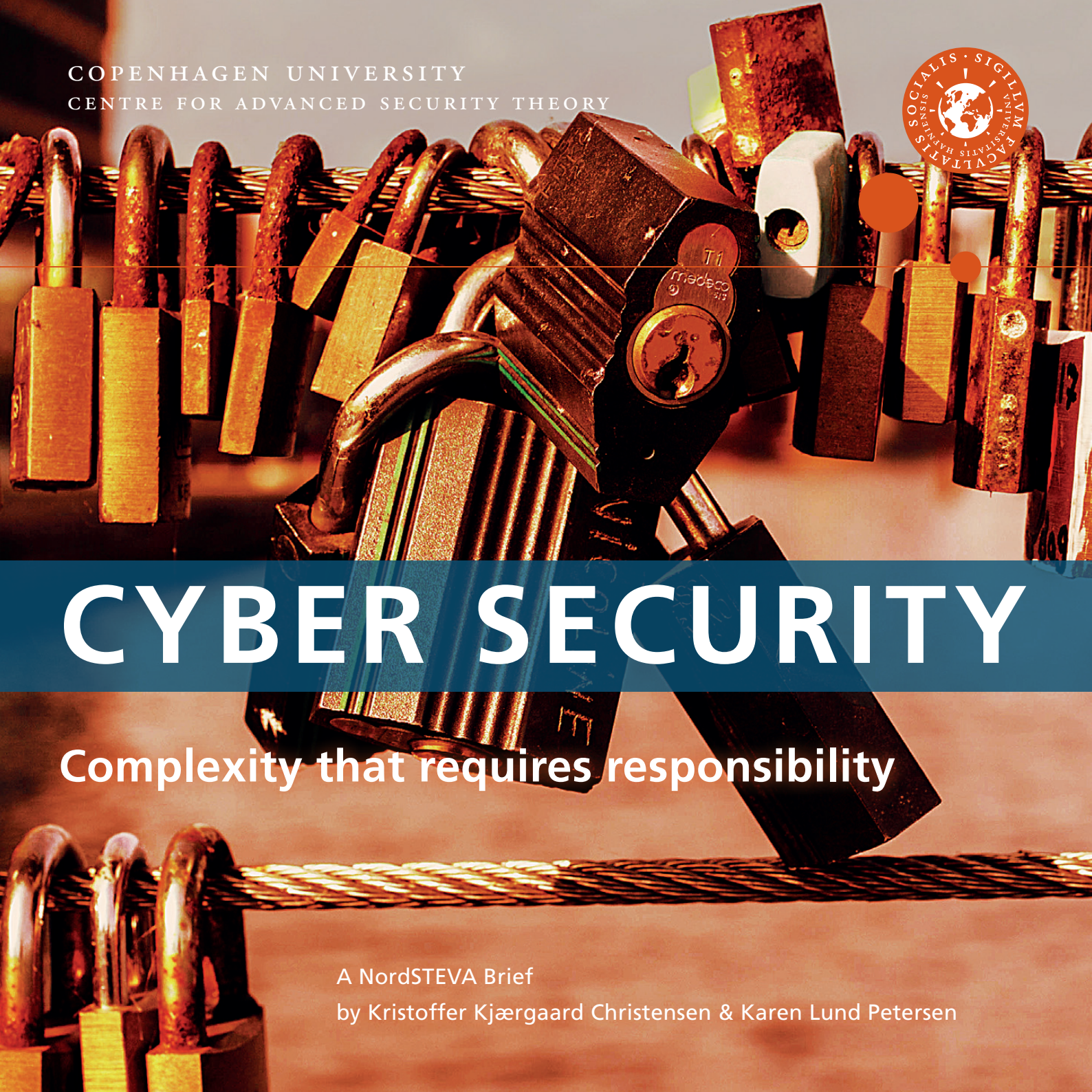
PhD Fellow Kristoffer Kjærgaard Christensen *(kk@ifs.ku.dk),*
Department of Political Science, University of Copenhagen.

Associate Professor Karen Lund Petersen *(klp@ifs.ku.dk),*
Department of Political Science, University of Copenhagen.

A Danish version of the argument has previously been presented in a paper published by the Danish Think Tank "Ret og Sikkerhed", It can be found at cast.ku.dk (Christensen and Petersen 2017a). The Danish version also introduced the Danish political and institutional framework for countering cyber threats.

Graphics and photography: SIGNS & WONDERS

COPENHAGEN UNIVERSITY
CENTRE FOR ADVANCED SECURITY THEORY



CYBER SECURITY

Complexity that requires responsibility

A NordSTEVA Brief

by Kristoffer Kjærgaard Christensen & Karen Lund Petersen